d)

(AJ)

(excerpt translation)

Japanese Pat. Appl. Laid-Open (kokai) No. HEI 11-167533
Laid-Open (kokai) Date: June 22, 1999
Title of the Invention: ELECTRONIC-MAIL FIREWALL DEVICE
Application No.: HEI 9-333239
Application Date: December 3, 1997
Applicant: TOSHIBA INFORMATION SYSTEMS CORPORATION
TOSHIBA CORPORATION
Inventor(s): Masatoshi TOMIOKA
Int. Cl.^{6} G06F 13/00, 9/06,
H04L 12/54, 12/58

※※※

If a virus is found in the e-mail, the e-mail firewall device refuses to receive the infected e-mail.

[0010]

[PREFERRED EMBODIMENT] A preferred embodiment of the present invention will now be described with reference to the accompanying drawings. FIG. 1 is a diagram schematically showing system configuration of an e-mail firewall device; a plurality of client computers 2 are connected to a mail server 1. E-mail firewall software 3, virus check software 4, and e-mail client software 5, as software constitute the e-mail firewall device, are installed in the respective client computers 2. The individual client computer 2 is equipped with an address registration database 6, and is connected with a monitor 7 and a keyboard (including a mouse or other pointing device) 8, which are used as interfaces for registering, in the address registration database, information as to whether an e-mail is receivable or not by the client computer 2.

[0011]

The e-mail firewall software 3 has functions of registration and collation by co-operating with the address registration database 6. Namely, the e-mail firewall software 3 collates the address of an e-mail sent to the client computer 2 with addresses (combinations of a user name and a domain name) from which the user of the client computer does not want to receive e-mails and which is registered in the address registration database 6, and adds an e-mail address to the address registration database 6 as required. The e-mail firewall software 3 has an address registration module for registering, using a GUI (graphical user interface), an address from which the user does not

want to receive an e-mail. For the purpose of previous check for virus infection, the e-mail firewall software 3 has also an extracting tool for a compressed file, a decoding tool for an encoded file, and an API (application program interface) for automatically starting the external virus check software 4.

[0012]

FIG. 2 is a diagram schematically showing a function of the e-mail firewall software 3. The e-mail firewall software 3 comprises a mail reception processing section 3a, a mail analyzing section 3b, a mail outputting section 3c, an extract processing section 3d, a decoder 3e, and a virus checker starting section 3f. The mail reception processing section 3a receives an e-mail, which is sent form the mail server 1, addressed to the user of the client computer 2; the mail analyzing section 3b analyzes a received e-mail to obtain a sender address, discriminate as to whether the received e-mail has an attached file, and further discriminate the file format of the attached file, i.e., whether the attached file is compressed and encoded; the mail outputting section 3c passes the received e-mail to the e-mail client software 5 when it is determined that the received e-mail is safe and is not set to receipt refusal; the mail extracting section 3d extracts an attached file to the e-mail if the mail analyzing section 3b has been discriminate that the file is compressed; the decoder 3e decodes the attached file when the mail analyzing section 3d has been discriminates that the file is encoded; the virus checker starting section 3f starts the virus check software 4 for checking as to whether the extracted or decoded file is infected by a virus or not.

[0013]

The e-mail firewall software 3 further comprises a database registering section 3g for registering an address on which the receipt refusal is set, in the address database 6 using the GUI, and a database collating section 3h for collating the sender address, which has been obtained by the mail analyzing section 3b, with e-mail addresses previously registered in the address registration database 6.

[0014]

An operation performed by the e-mail firewall device will now be described with reference to a flow diagram of FIG. 3. First of all, prior to receiving an e-mail from the mail server, the user of the client computer 2 starts the address registration module of the e-mail firewall software 3 if necessary. Then the user operates the monitor 7 and the keyboard 8, and registers an address from which the user does not want to receive an e-mail so that the address is registered in the address registration database 6 as a receipt refusal address (step S1).

[0015]

When the client computer 2 receives an e-mail from the mail server 1 (step S2), the sender address of the received e-mail is checked out and is collated with receipt refusal address in the address registration database 6 (step S3). If it is determined that the address of the received e-mail is a receipt refusal address (step S4), an action for a receipt refusal address is executed and a pop-up window, on which the sender address and a select button, such as ignore, return, or send template (e.g., "I refuse to receive your e-mail. Please send me no e-mail anymore."), is displayed on the monitor 7 of the client computer 2 for the user's selection (steps S5, S6).

[0016]

On the other hand, if it is determined that the address of the received e-mail is not a receipt refusal address by the collation in step S3 (NO route of step S4), it is discriminated as to whether the received e-mail has an attached file (step S7). Subsequently, when the received e-mail does not have an attached file, the e-mail is regarded as a safe e-mail and the received e-mail, which has been received from the mail server 1, is simply passed to the e-mail client software 5 (step S8).

[0017]

When it is discriminated that the received e-mail has an attached file at step S7, it is further discriminated as to whether the attached file is compressed or encoded. If the attached file is compressed, the file is extracted; and if encoded, the file is decoded (steps S9, S10).

[0018]

Then the virus check software 4 is started (step S11) to check as to whether the extracted or decoded file is infected by a virus or not. If it is determined that the file is virus-free, the e-mail, which is received from the mail server 1, is simply passed to the e-mail client software 5 as a safe e-mail (steps S12, S18). On the other hand, if a virus is found in the file, the user is notified of the detection of the virus through a pop-up window on the monitor 7 so that the user makes an operation to remove the virus out of the file (step S13).

(d)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-167533
(43)Date of publication of application : 22.06.1999

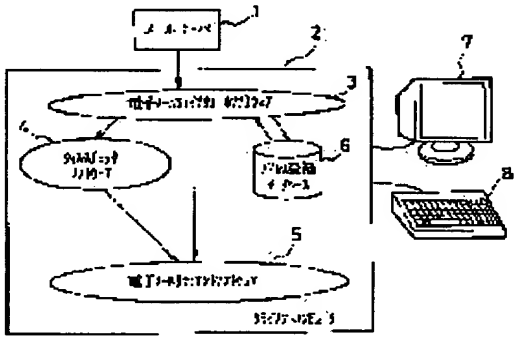
(51)Int.Cl. G06F 13/00
G06F 9/06
H04L 12/54
H04L 12/58

(21)Application number : 09-333239
(22)Date of filing : 03.12.1997

(71)Applicant : TOSHIBA INFORMATION SYSTEMS CORP
TOSHIBA CORP
(72)Inventor : TOMIOKA MASATOSHI

(54) ELECTRONIC MAIL FIREWALL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To select received mails so as to receive only virus-free mails by automatically checking junk mails for rejection, and automatically making a virus check on mails judged to be accepted and then receiving them.
SOLUTION: This electronic mail firewall device 3 collates in advance an electronic mail delivered from a mail server 1 against an address registration data base 6 on the side of a client computer 2, and an electronic mail sent from a mail address where reception rejection is set is rejected and not saved in a mail box 5. Even for an electric mail sent from a mail address where the reception rejection is not set, API starts virus check application software 4 to make a virus check and the electronic mail containing a virus is rejected.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(d)

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１１－１６７５３３

(43)公開日　平成11年(1999)6月22日

(51)Int. Cl.[6]		識別記号	FI		
G06F	13/00	351	G06F	13/00	351 G
					351 Z
	9/06	550		9/06	550 Z
H04L	12/54		H04L	11/20	101 B
	12/58				

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平9-333239

(22)出願日　平成9年(1997)12月3日

(71)出願人　391016358
東芝情報システム株式会社
神奈川県川崎市川崎区日進町7番地1

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　冨岡　正俊
神奈川県川崎市川崎区日進町7番地1　東芝情報システム株式会社内

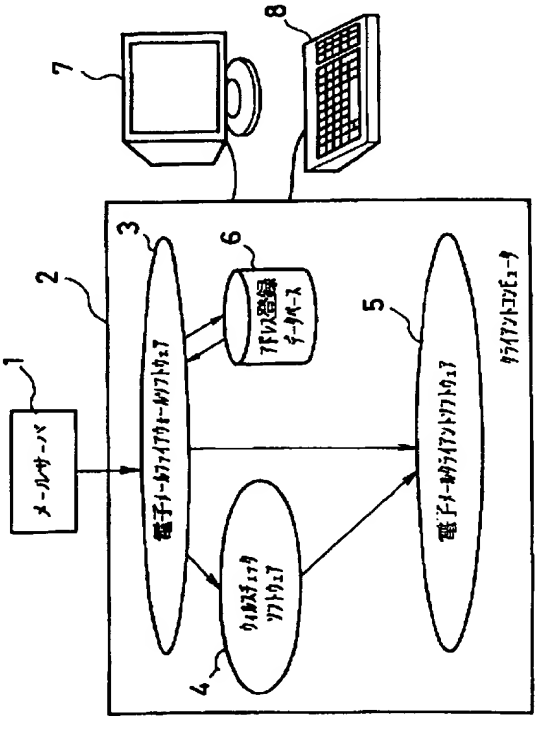
(74)代理人　弁理士　三好　秀和　（外1名）

(54)【発明の名称】電子メールファイアウォール装置

(57)【要約】

【課題】　ジャンクメールを自動的にチェックして受取り拒否し、かつ受取ることにしたメールに対してもウィルスチェックを自動的に実行してから受取るようにして、受信メールを選別し、かつウィルスフリーのメールのみ受け取る。

【解決手段】　この電子メールファイアウォール装置３は、メールサーバ１から配信されてきた電子メールに対して、クライアントコンピュータ２側であらかじめアドレス登録データベース６と照合し、受取り拒否の設定がされているメールアドレスから送信されて来た電子メールは受取り拒否してメールボックス５に保存させない。また受取り拒否の登録がされていないメールアドレスから送信されて来た電子メールに対しても、ＡＰＩがウィルスチェックアプリケーションソフトウェア４を起動させてウィルスチェックを実行させてウィルスの混入している電子メールであれば受取りを拒否する。



1

【特許請求の範囲】

【請求項１】　受取り拒否すべきメールアドレスを登録したアドレス登録データベースと、

前記アドレス登録データベースに対して受取り拒否すべきメールアドレスを登録するためのユーザインタフェースと、

メールサーバから受取った電子メールに対して、その送信元メールアドレスを前記アドレス登録データベースと照合し、受取り拒否の登録がされているメールアドレスから送られて来た電子メールの受取りを拒否する受取り拒否判定手段と、

前記受取り拒否判定手段が受取り拒否しなかった電子メールに対して、外部ウィルスチェックアプリケーションソフトウェアを起動させるアプリケーションプログラムインタフェース（ＡＰＩ）とを備えて成る電子メールファイアウォール装置。

【請求項２】　前記受取り拒否判定手段が受取り拒否した電子メールをその送信元に返送するメール返送手段を備えて成る請求項１に記載の電子メールファイアウォール装置。

【請求項３】　前記ＡＰＩが、圧縮ファイルに対する解凍処理機能、及び／又はエンコードファイルに対するデコード処理機能を有することを特徴とする請求項１又は２に記載の電子メールファイアウォール装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はジャンクメールを自動的に選別して受取り拒否するための電子メールファイアウォール装置に関する。

【０００２】

【従来の技術】近年、インターネットの発展でだれでもメールアドレスを取得すれば、インターネットに接続して電子メール（Ｅ－Ｍａｉｌ）の送受ができるようになってきている。

【０００３】

【発明が解決しようとする課題】ところが、電子メールの場合、送信先のメールアドレス、つまりドメインアドレスが判明していれば誰でも自由に任意のメッセージを作成して送信できるため、悪意を持った第三者が無差別にメールを配信してトラフィックを増大させたり、また添付ファイルにウィルスを混入させて配信して送信先のコンピュータにウィルスを侵入させる問題点があった。またダイレクトメール企業が製品売込みのために一方的に広告メールを配信することにより、受信メール中に多数の不要なメール（ジャンクメール）が蓄積され、重要なメールを見落としてしまう危険性もあった。

【０００４】本発明はこのような従来の問題点に鑑みてなされたもので、ジャンクメールをその受取り窓口で自動的にチェックして受取り拒否し、かつ受取ることにしたメールに対してもウィルスチェックを自動的に実行してからでないと受取らないようにして受信メールを選別し、かつウィルスフリーのメールのみが受け取れるようにした電子メールファイアウォール装置を提供することを目的とする。

2

【０００５】本発明はまた、送信元に受取り拒否の態度を表明するために自動的にジャンクメールをその送信元に返送することができる電子メールファイアウォール装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】請求項１の発明の電子メールファイアウォール装置は、受取り拒否すべきメールアドレスを登録したアドレス登録データベースと、前記アドレス登録データベースに対して受取り拒否すべきメールアドレスを登録するためのユーザインタフェースと、メールサーバから受取った電子メールに対して、その送信元メールアドレスを前記アドレス登録データベースと照合し、受取り拒否の登録がされているメールアドレスから送られて来た電子メールの受取りを拒否する受取り拒否判定手段と、前記受取り拒否判定手段が受取り拒否しなかった電子メールに対して、外部ウィルスチェックアプリケーションソフトウェアを起動させるアプリケーションプログラムインタフェース（ＡＰＩ）とを備えたものである。

【０００７】請求項１の発明の電子メールファイアウォール装置では、ユーザがユーザインタフェースを用いてアドレス登録データベースに受取り拒否したいメールアドレスをあらかじめ登録しておく。そしてメールサーバから配信されてきた電子メールに対して、クライアントコンピュータ側であらかじめアドレス登録データベースと照合し、受取り拒否の設定がされているメールアドレスから送信されて来た電子メールは受取り拒否してメールボックスに保存させない。また受取り拒否の登録がされていないメールアドレスから送信されて来た電子メールに対しても、ＡＰＩがウィルスチェックアプリケーションソフトウェアを起動させてウィルスチェックを実行させてウィルスの混入している電子メールであれば受取りを拒否する。こうしてジャンクメールを除き、ウィルスフリーの電子メールのみを選択してクライアントコンピュータのメールボックスに保存する。

【０００８】請求項２の発明は、請求項１の電子メールファイアウォール装置において、さらに、前記受取り拒否判定手段が受取り拒否した電子メールをその送信元に返送するメール返送手段を備えたものであり、受取り拒否する電子メールを返送することによって送信元に受取り拒否の態度を明確に知らせ、再度送信されて来ることがないようにする。

【０００９】請求項３の発明は、請求項１又は２の電子メールファイアウォール装置において、前記ＡＰＩが圧縮ファイルに対する解凍処理機能、及び／又はエンコードファイルに対するデコード処理機能を有するものであ

り、電子メールに添付されているファイルが圧縮ファイルであれば解凍処理してウィルスチェックし、またエンコードされているファイルであればデコード処理してウィルスチェックし、ウィルスが混入されているファイルであれば受取り拒否することにより、メールボックスに保存する電子メールの安全性を高める。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を図に基づいて詳説とする。図１は本発明の電子メールファイアウォール装置のシステム構成を示しており、メールサーバ１に対して複数のクライアントコンピュータ２がネットワーク接続されている。そしてこのクライアントコンピュータ２において、本発明の電子メールファイアウォール装置を構成するソフトウェアとして電子メールファイアウォールソフトウェア３と、ウィルスチェックソフトウェア４と、電子メールクライアントソフトウェア５がセットアップされており、アドレス登録データベース６が備えられ、さらに、このアドレス登録データベース６に対してメール受取り可不可の登録をするためのユーザインタフェースとして表示装置７及びキーボード（マウスその他のポインティングデバイスも含む）８が接続されている。

【００１１】電子メールファイアウォールソフトウェア３はアドレス登録データベース６と連動する登録／照合機能を持ち、アドレス登録データベース６に登録されている受取りたくないメールアドレス（ユーザ名とドメイン名とから構成される）の登録と配信されて来た電子メールのメールアドレスとを照合し、必要があればメールアドレスの追加登録を行う。電子メールファイアウォールソフトウェア３はまた、ＧＵＩ（グラフィカルユーザインタフェース）を用いてアドレス登録データベース６に受取りたくないメールアドレスを登録するためのアドレス登録モジュールを実装し、さらに、受取ろうとする電子メールに対して、その添付ファイルに混入するウィルスを事前にチェックするために、圧縮ファイルに対する解凍ツール及びエンコードファイルに対するデコードツール、そして外部のウィルスチェックソフトウェア４を自動起動させるＡＰＩ（アプリケーションプログラムインタフェース）を持っている。

【００１２】図２はこの電子メールファイアウォールソフトウェア３の機能構成を示しており、メールサーバ１から配信される自クライアントアドレス宛の電子メールの受取り処理を行うメール受取り処理部３ａ、受取った電子メールを解析し、送信元メールアドレス、添付ファイルの有無、添付ファイルのファイル形式、すなわち、圧縮ファイルかエンコードファイルかを判別するメール解析部３ｂ、受取ったメールが安全であり、かつ受取り拒否設定されていない送信元アドレスからのメールである時にその電子メールを電子メールクライアントソフトウェア５に受け渡すメール出力部３ｃ、メール解析部３ｂで電子メールに添付されたファイルが圧縮ファイルであると判明した場合にその解凍処理を行う解凍処理部３ｄ、またメール解析部３ｂで電子メールに添付されたファイルがエンコードされたファイルであると判明した場合にデコードするデコーダ３ｅ、これらの解凍ファイル又はデコードファイルのウィルスチェックを行うウィルスチェックソフトウェア４を起動するウィルスチェッカ起動部３ｆを有している。

【００１３】電子メールファイアウォールソフトウェア３はまた、アドレス登録データベース６に対してＧＵＩを用いて受取り拒否アドレスの登録処理を行うデータベース登録処理部３ｇ、メール解析部３ｂで抽出した送信元メールアドレスをこのアドレス登録データベース６に登録されているメールアドレスと照合するデータベース照合処理部３ｈを備えている。

【００１４】次に、上記構成の電子メールファイアウォール装置の動作を、図３のフローチャートを用いて説明する。ユーザはメールサーバ１からの配信を受ける前に、必要に応じて電子メールファイアウォールソフトウェア３のアドレス登録モジュールを立上げ、表示装置７及びキーボード８を用い、ＧＵＩを利用して受信したくないメールアドレスを受取り拒否アドレスとしてアドレス登録データベース６に登録する（ステップＳ１）。

【００１５】そしてメールサーバ１から実際に配信があった場合には（ステップＳ２）、受取った電子メールに対してその送信元のメールアドレスをチェックし、アドレス登録データベース６に登録されている受取り拒否アドレスと照合する（ステップＳ３）。ここで受取り拒否アドレスとして登録されているメールアドレスからの電子メールであれば（ステップＳ４）、受取り拒否アクションを実行し、クライアントコンピュータ２の表示装置７にポップアップウィンドウにして、送信元メールアドレスと共に、無視／返送／登録されている文章（例えば、「受取りを拒否します。今後、送信しないで下さい。」といった文章）の返信の選択ボタンを表示してユーザに選択させる（ステップＳ５，Ｓ６）。

【００１６】またステップＳ３の照合で、データベース６に登録されていないメールアドレスからの電子メールであれば（ステップＳ４でＮＯに分岐）、添付ファイルがあるかどうか判別し（ステップＳ７）、添付ファイルがなければ安全な電子メールであるとみなして電子メールクライアントソフトウェア５にメールサーバ１から受取った電子メールをそのまま渡す（ステップＳ８）。

【００１７】しかしながら、ステップＳ７で添付ファイルありと判別すれば、その添付ファイルが圧縮又はエンコードされたファイルであるかどうか判別し、圧縮ファイルであれば解凍処理し、またエンコードファイルであればデコードする（ステップＳ９，Ｓ１０）。

【００１８】そして添付ファイルについてウィルスチェックソフトウェア４を起動し（ステップＳ１１）、ウィ

ルスを発見しなければ安全な電子メールとして電子メールクライアントソフトウェア５にメールサーバ１から受取った電子メールをそのまま渡す（ステップＳ１２，Ｓ８）。しかしながら、ウィルスを発見した場合には、クライアントコンピュータ２の表示装置７にポップアップウィンドウを用いてウィルス発見を表示してユーザに知らせ、ウィルス除去作業を行わせるようにする（ステップＳ１３）。

【００１９】このようにしてこの実施の形態の電子メールファイアウォール装置では、メールサーバ１から電子メールの配信を受けた場合に実際の電子メールクライアントソフトウェアによる通常の受信処理を行う前に、送信元メールアドレスをチェックして受信拒否登録してあればその受取りを拒否して、いわば門前払いの形で電子メールクライアントソフトウェアにジャンクメールが多数蓄積されるのを防止し、クライアントコンピュータのユーザの作業能率を向上させることができ、同時にトラフィックの軽減も図ることができる。またウィルスが混入されているようなファイルが添付されている悪意の電子メールに対しても電子メールクライアントソフトウェアにより受信処理する前にチェックしてウィルス侵入を防止することができる。

【００２０】

【発明の効果】以上のように請求項１の発明によれば、ジャンクメールを除き、ウィルスフリーの電子メールのみを選択してクライアントコンピュータのメールボックスに保存することができ、ユーザの電子メールを読む時間を短縮し、また電子メールソフトウェアに保存される前にウィルスの侵入をシャットアウトすることができてシステムの信頼性を高めることができる。

【００２１】請求項２の発明によれば、受取り拒否する電子メールを返送するので、送信元に受取り拒否の態度を明確に知らせ、再度送信されて来ることがないようにすることができる。

【００２２】請求項３の発明によれば、電子メールに添付されているファイルが圧縮ファイルであれば解凍処理してウィルスチェックし、またエンコードされているファイルであればデコード処理してウィルスチェックし、ウィルスが混入されているファイルであれば受取り拒否することにより、メールボックスに保存する電子メールの安全性を高めることができる。

【図面の簡単な説明】

【図１】本発明の１つの実施の形態のシステム構成を示すブロック図。

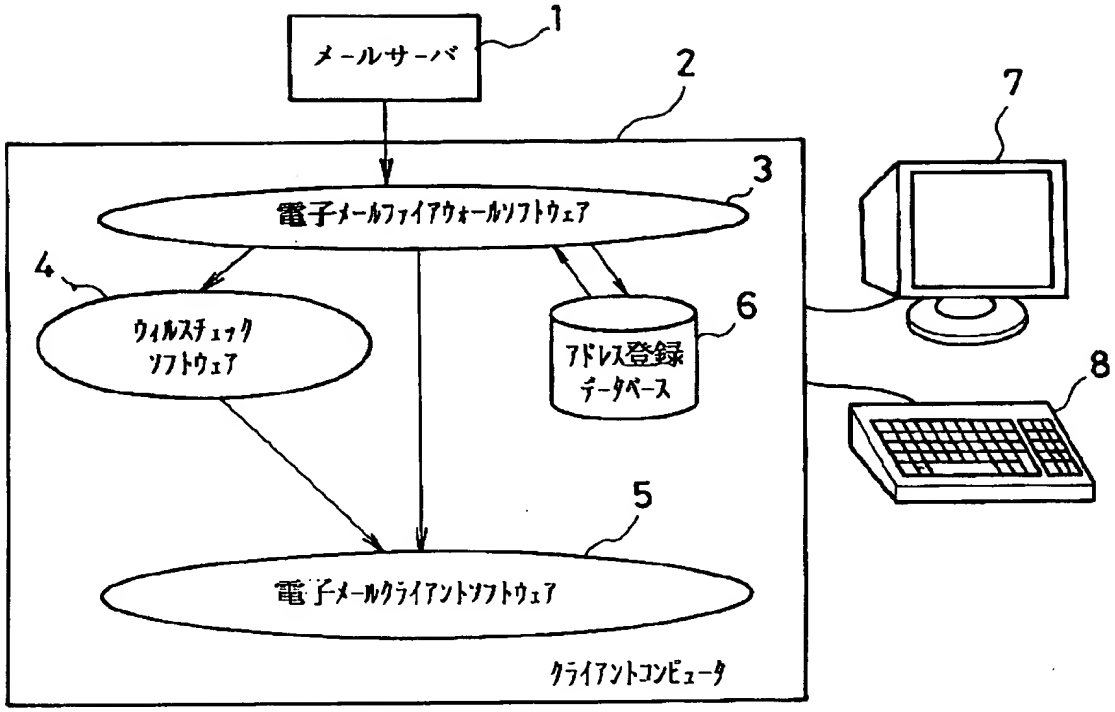
【図２】上記の実施の形態で実行する電子メールファイアウォールソフトウェアの機能構成を示すブロック図。

【図３】上記の実施の形態の処理動作を示すフローチャート。

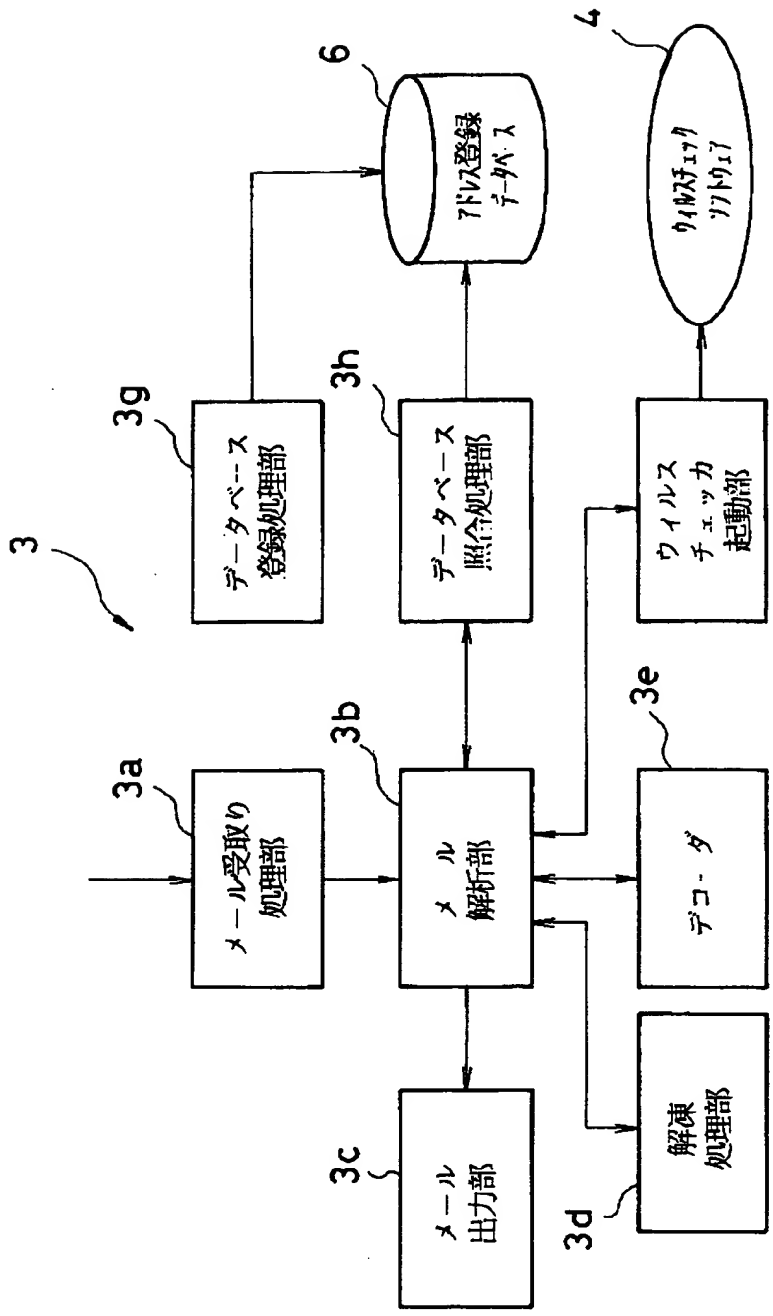
【符号の説明】

１　メールサーバ
２　クライアントコンピュータ
３　電子メールファイアウォールソフトウェア
４　ウィルスチェックソフトウェア
５　電子メールクライアントソフトウェア
６　アドレス登録データベース
７　表示装置
８　キーボード

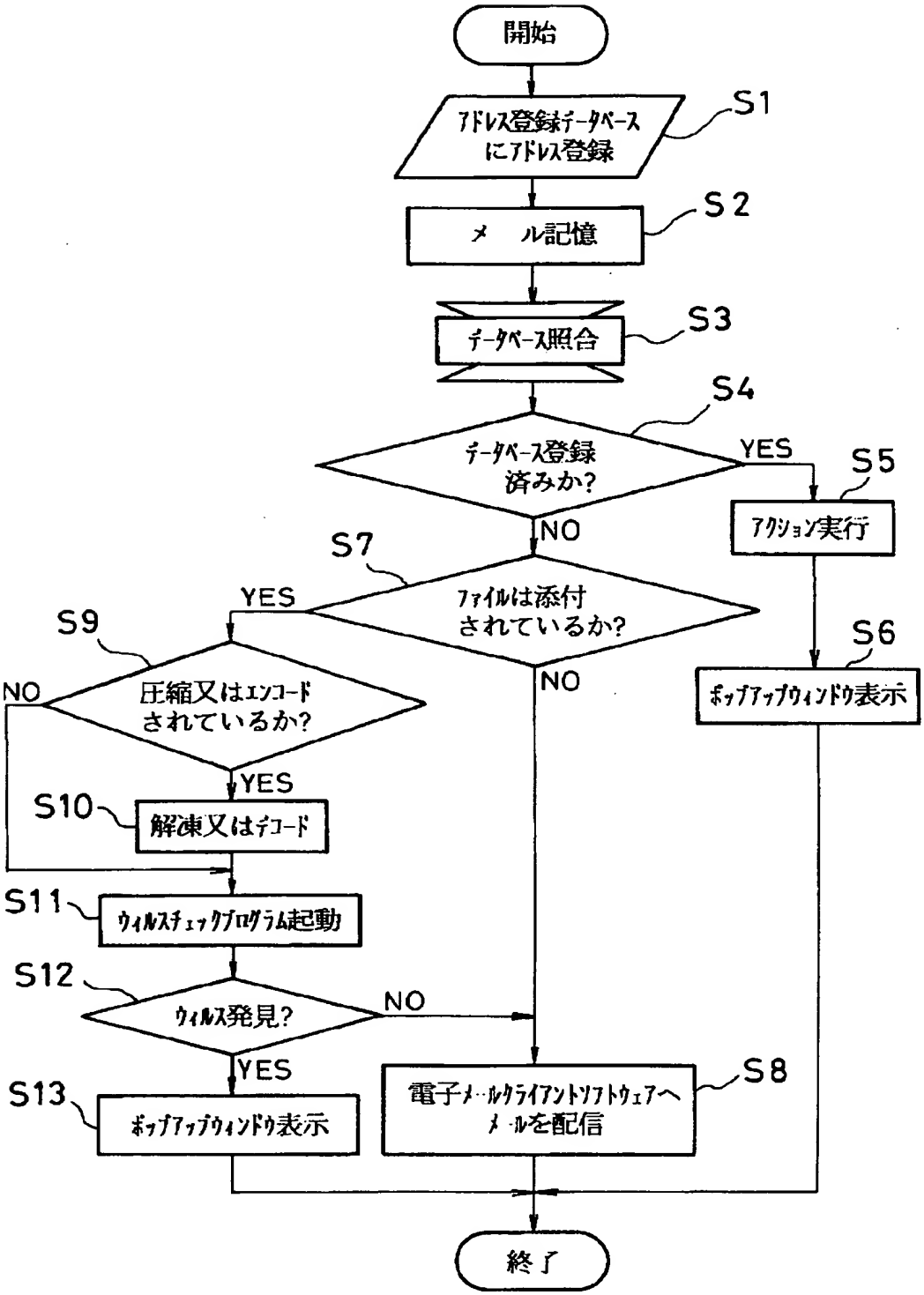
【図１】


メールサーバ
1
2
7
3
電子メールファイアウォールソフトウェア
4
ウィルスチェック
ソフトウェア
アドレス登録
データベース
6
8
5
電子メールクライアントソフトウェア
クライアントコンピュータ

【図２】


3
3a
メール受取り処理部
3b
メール解析部
3c
メール出力部
3d
解凍処理部
3e
デコーダ
3g
データベース登録処理部
3h
データベース照合処理部
ウィルスチェッカ起動部
6
アドレス登録データベース
4
ウィルスチェッカソフトウェア

【図３】


開始
アドレス登録データベースにアドレス登録
S1
メール記憶
S2
データベース照合
S3
S4
データベース登録済みか?
YES
S5
アクション実行
NO
S7
ファイルは添付されているか?
YES
S9
NO
圧縮又はエンコードされているか?
S6
ポップアップウィンドウ表示
NO
YES
S10
解凍又はデコード
S11
ウィルスチェックプログラム起動
S12
ウィルス発見?
NO
YES
S13
ポップアップウィンドウ表示
電子メールクライアントソフトウェアへメールを配信
S8
終了